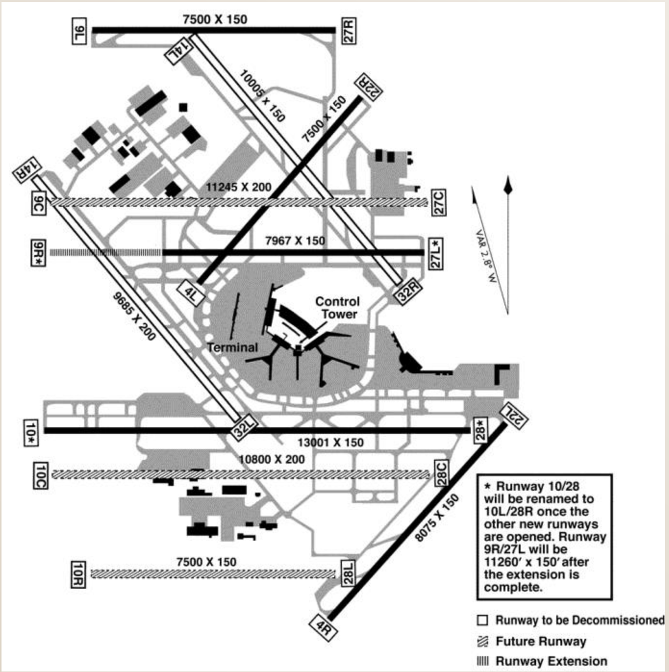
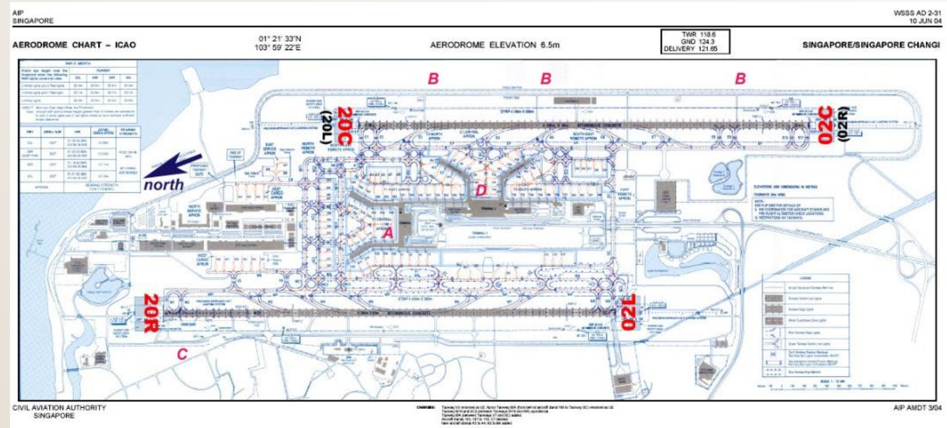
Temporal Precedence Checking for Switched Models and Its Application to a Parallel Landing Protocol

Parasara Sridhar Duggirala,
Le Wang,
Sayan Mitra,
Mahesh Viswanathan, and
Cesar Munoz

ILLINOIS



Chicago O'Hare International Airport

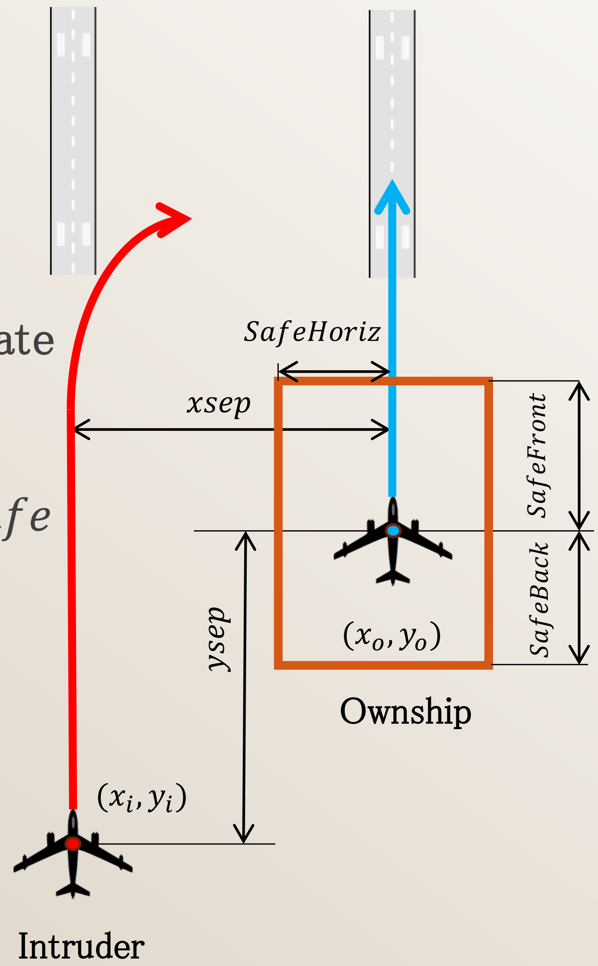


Singapore Changi International Airport

- Airports with multiple runways
- FAA pushing for a parallel landing mechanism – SAPA
- Requires an alerting mechanism - ALAS developed by NASA
- Verifying the validity of alerting mechanism

Parallel Landing: A Case Study

- *Ownship* and *Intruder* perform parallel landing
- Malicious behavior of intruder – turns towards the ownship while landing
- Alert mechanism to warn ownship: **guarantee predicate**
- Property of interest Alert is generated before Unsafe
- Challenges in verification
  - Verifying temporal precedence
  - Predicates based on projected future behavior



Contributions

- Verification technique for temporal precedence properties
- Verifying guarantee predicates
- Application to Adjacent Landing Alerting System (ALAS) for checking $Alert \prec_b Unsafe$ property

Checking temporal precedence property with guarantee predicates and apply it to ALAS system

Overview

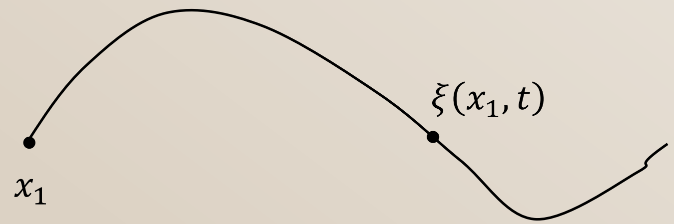
- ✓ Motivation
- System Model and Properties
- Temporal Precedence Property Verification
  - Reachable set computation using annotations
  - Temporal precedence checking
  - Verifying guarantee predicates
- ALAS system and verification results

System Model

- Switched System Model
- System dynamics $\dot{x} = f(x)$, solution is $\xi(x_0, t)$

$$\frac{d}{dt}\xi(x_0, t) = f(\xi(x_0, t))$$

- Multiple modes of operation $\{ f_i \mid i \in I \}$
- Switching signal $\sigma : \mathrm{R}^{\geq 0} \rightarrow I$ denotes the switching among modes

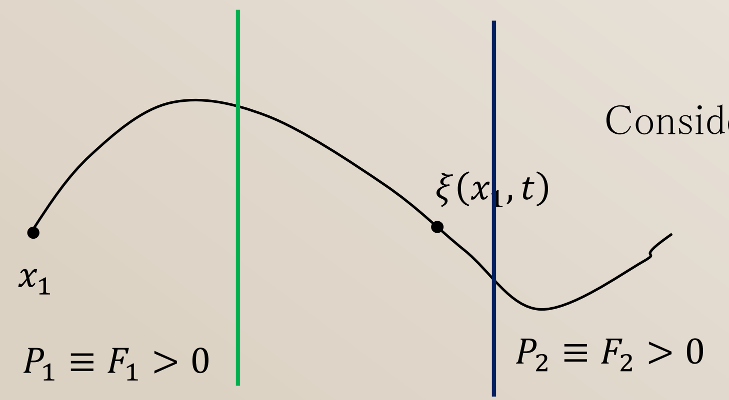


Temporal Precedence Property

- Predicate $P \subseteq \mathbb{R}^n$ is satisfied by ξ from x_0 at time t iff $\xi(x_0, t) \in P$

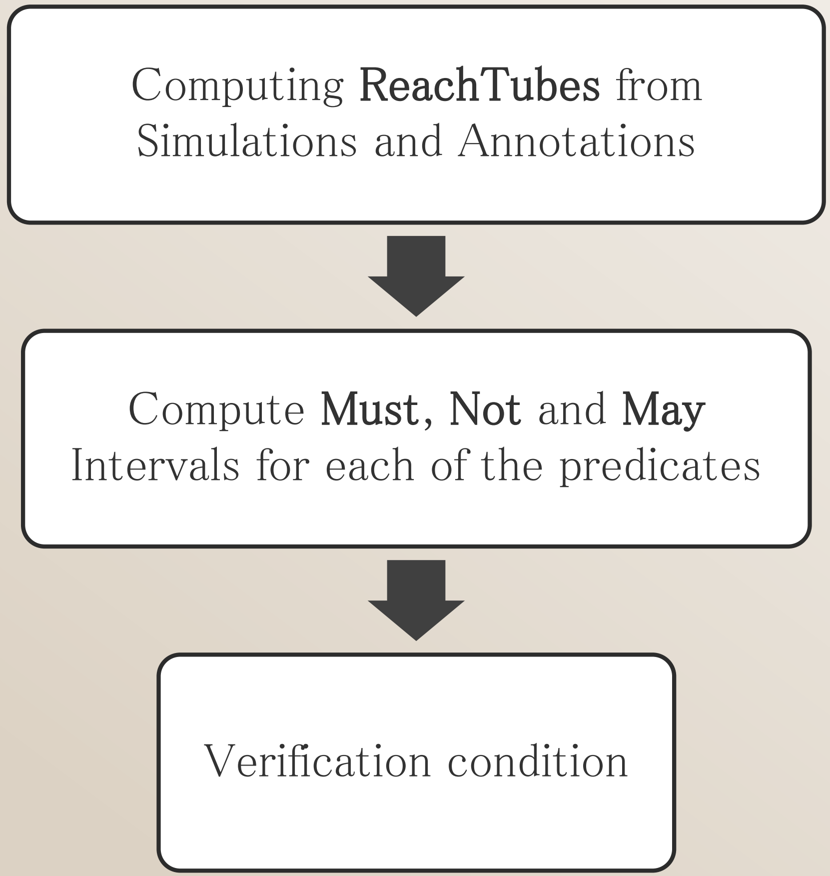
- Temporal precedence property $P_1 \prec_b P_2$ is satisfied by ξ from x_0 iff
$$\forall t, P_2(\xi(x_0, t)) = \top, \exists\, t' < t - b, P_1\big(\xi(x_0, t')\big) = \top$$

- For ALAS, temporal precedence property $Alert \prec_b Unsafe$



Consider the temporal precedence property
$P_1 \prec_0 P_2$

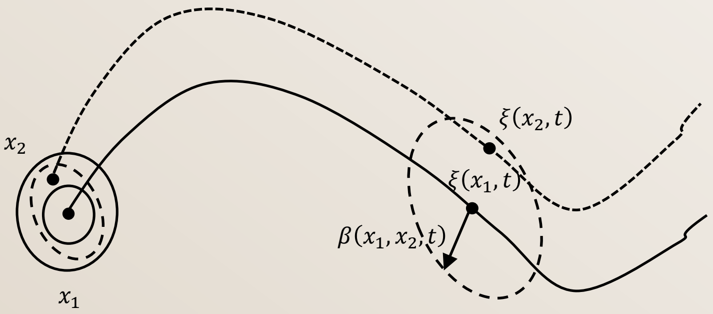
Temporal Precedence Verification



Computing *ReachTubes*

- Annotations – conservative upper bound among distance between trajectories
- Annotations for ODE $\dot{x} = f(x)$ is V, β such that

$$\forall t > 0, V\big(\xi(x_1, t), \xi(x_2, t)\big) \leq \beta(x_1, x_2, t)$$

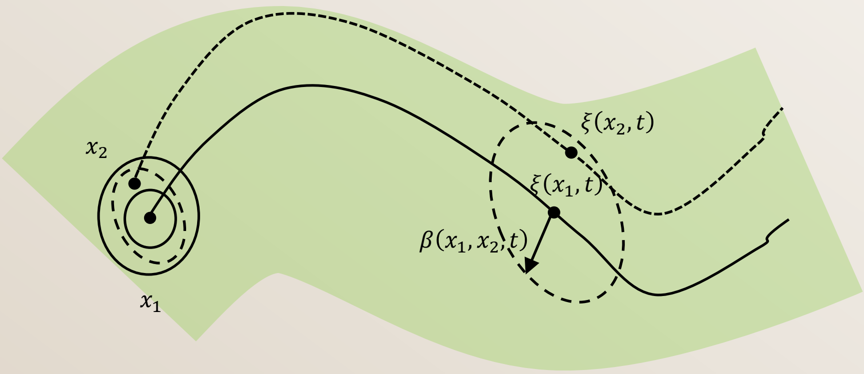


Verification of Annotated Models From Executions [DMV'13]

Computing *ReachTubes*

- Annotations - conservative upper bound among distance between trajectories
- Annotations for ODE $\dot{x} = f(x)$ is V, β such that

$$\forall t > 0, V\big(\xi(x_1, t), \xi(x_2, t)\big) \leq \beta(x_1, x_2, t)$$



- Utility of annotation:

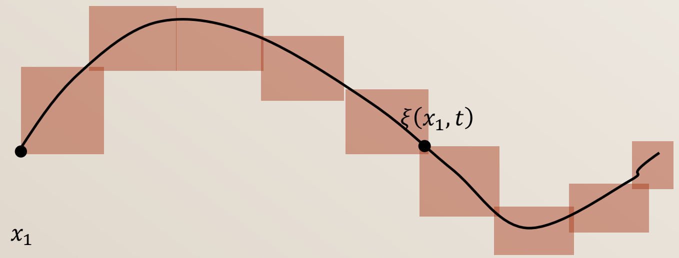
$$\boldsymbol{\xi(y, t) \in Bloat_{\epsilon}(\xi(x, t))} \text{ where } \boldsymbol{\epsilon} = \sup_{\boldsymbol{y \in B_{\delta}(x)}} \{\boldsymbol{\beta(x, y, t)}\}$$

Verification of Annotated Models From Executions [DMV'13]

ReachTubes From Simulations And Annotations

- $\xi(x_0, t)$ - general analytical solution does not exist
- Validated simulation engines generate regions for time intervals

$$\rho = (R_1, [t_0, t_1]), \ldots, (R_l, [t_{l-1}, t_l]), \forall t \in [t_{i-1}, t_i], \xi(t) \in R_i$$

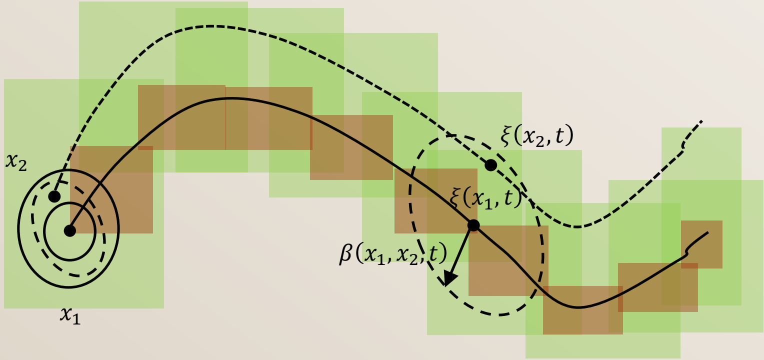


ReachTubes From Simulations And Annotations

- $\xi(x_0, t)$ - general analytical solution does not exist
- Validated simulation engines generate regions for time intervals

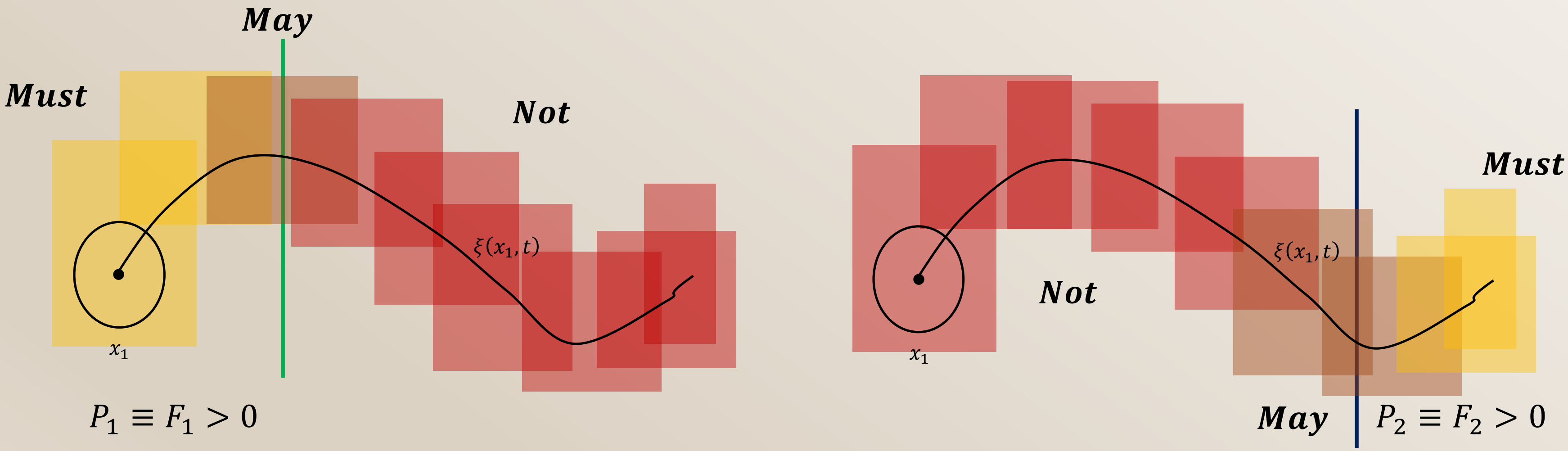
$$\rho = (R_1, [t_0, t_1]), \dots, (R_l, [t_{l-1}, t_l]), \forall t \in [t_{i-1}, t_i], \xi(t) \in R_i$$

- *ReachTube* $\psi = B_\epsilon(\rho)$ where $\epsilon = \sup_{y \in B_\delta(x)} \{\beta(x, y, t)\}$
- Overapproximation can be made arbitrarily small
- How to infer temporal properties from such *ReachTubes*



Must, Not, and May Intervals

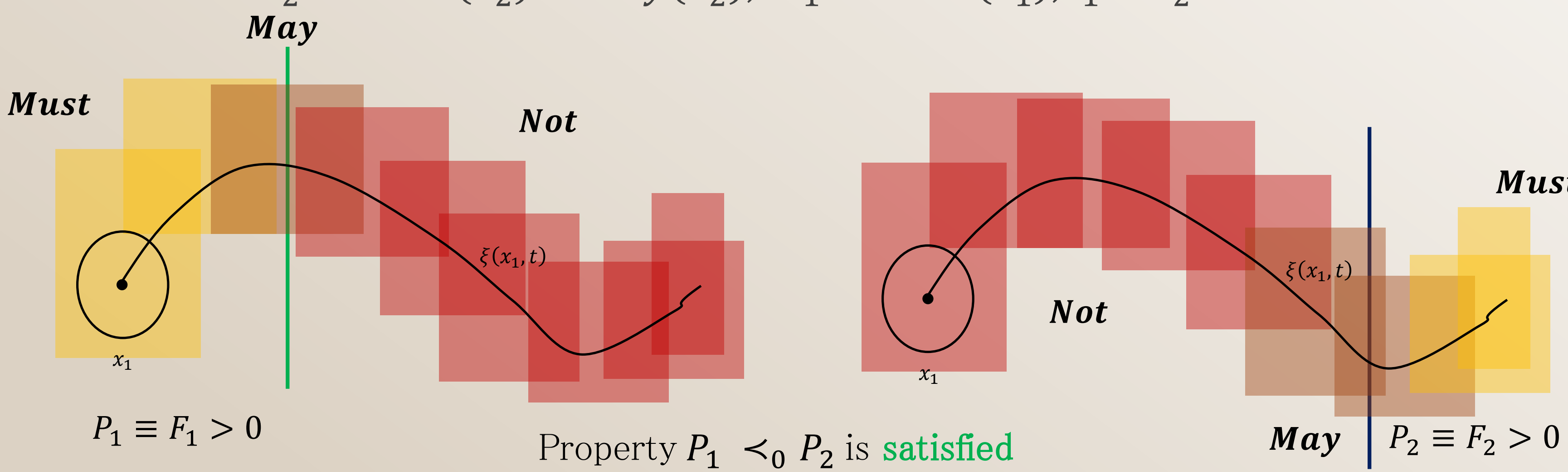
- For a predicate P, and *ReachTube* $\psi = (O_1, [t_0, t_1]), \ldots, (O_l, [t_{l-1}, t_l])$ the interval $[t_{i-1}, t_i]$ is
  - in $Must(P)$ if $O_i \subseteq P$
  - in $Not(P)$ if $O_i \cap P = \emptyset$
  - in $May(P)$ otherwise



Checking Temporal Precedence

- Temporal precedence $P_1 \prec_b P_2$ is satisfied by *ReachTube* ψ if

$$\forall I_2 \in Must(P_2) \cup May(P_2), \exists I_1 \in Must(P_1), I_1 < I_2 - b$$



Property $P_1 \prec_0 P_2$ is satisfied

- Temporal precedence $P_1 \prec_b P_2$ is violated by *ReachTube* ψ if

$$\exists I_2 \in Must(P_2), \forall I_1 \in Must(P_1) \cup May(P_1), I_1 > I_2 - b$$

Soundness and Relative Completeness

- *ReachTubes* can be made arbitrarily precise by
  1. Decreasing the time step
  2. Finer partition of the initial set

- Algorithm for verifying temporal precedence
  1. Partition initial set, and compute *ReachTubes* for each partition
  2. If temporal precedence is satisfied by all *ReachTubes,* return **satisfied**
  3. If violated, return **not satisfied**, else refine the partitioning and time step

- If the algorithm returns **satisfied** (**not-satisfied**) then system satisfies (**violates**) the property. If the system **robustly satisfies** (**robustly violates**) the property, algorithm will terminate with correct answer.

Checking Guarantee Predicates

- **Assumption:** Checking $O \subseteq P$ or $O \subseteq P^c$ is trivial
- *Alert* predicate based on future behavior of aircraft
- Guarantee predicates with *lookahead* function L_P such that
$$P(x) \equiv \exists t, L_P(x,t) > 0$$
- If lookahead function is defined as solution of ODE, i.e.
$L_P \equiv w\big(\xi'(x,t)\big) > 0$ where ξ' is the solution to $\dot{x} = g(x)$

Checking Guarantee Predicates

- **Assumption:** Checking $O \subseteq P$ or $O \subseteq P^c$ is trivial
- *Alert* predicate based on future behavior of aircraft
- Guarantee predicates with *lookahead* function L_P such that
$$P(x) \equiv \exists t, L_P(x,t) > 0$$
- If lookahead function is defined as solution of ODE, i.e.
$$L_P \equiv w\big(\xi'(x,t)\big) > 0 \text{ where } \xi' \text{ is the solution to } \dot{x} = g(x)$$
- **Technique**: Compute *ReachTubes* for $\dot{x} = g(x)$ and check for $Must(w)$
- If $Must(w) \neq \emptyset$, guarantee predicate is <u>satisfied</u>
- If $Must(w) \cup May(w) = \emptyset$, guarantee predicate is <u>not satisfied</u>
- Else, compute finer *ReachTubes* and repeat

Overview

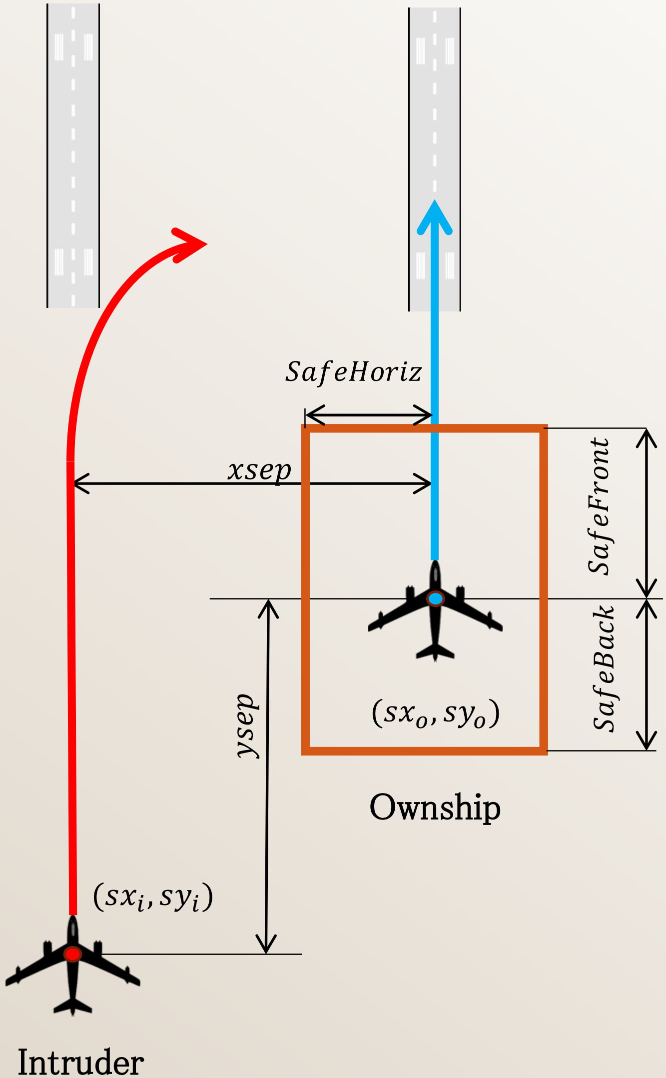
- ✓ Motivation
- ✓ System Model and Properties
- ✓ Temporal Precedence Property Verification
  - ✓ Reachable set computation using annotations
  - ✓ Temporal precedence checking
  - ✓ Verifying guarantee predicates
- ALAS system, properties and verification results

ALAS Protocol

- Parallel landing with separation between runways
- *Ownship* and *Intruder* aircraft
- Intruder behavior - 2 modes: *approach* and *turn*
  - *Approach* - Aircraft follows straight line trajectory to runway
  - *Turn* - Aircraft turns at bank angle ϕ_i

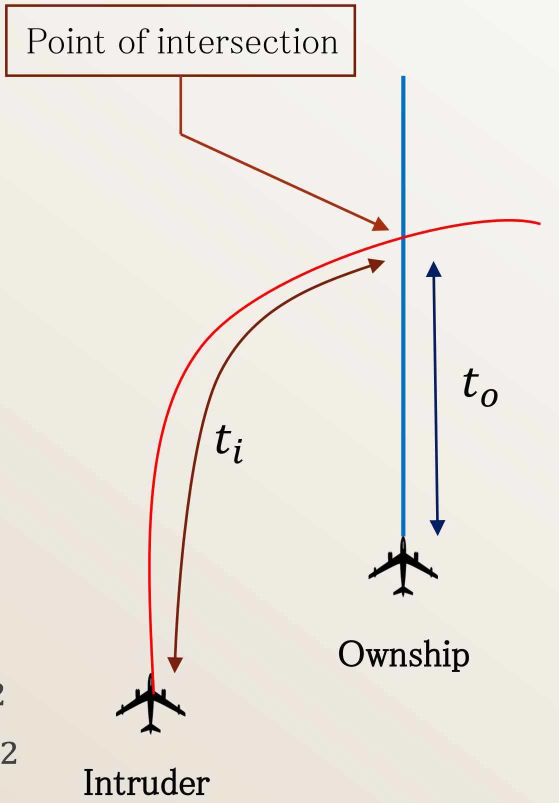
$$\begin{bmatrix} \dot{sx_i} \\ sy_i \\ vx_i \\ vy_i \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \omega_i \\ 0 & 0 & -\omega_i & 0 \end{bmatrix} \begin{bmatrix} sx_i \\ sy_i \\ vx_i \\ vy_i \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \omega_i - c_y \\ \omega_i + c_x \end{bmatrix}$$

where $\omega_i = \frac{G\,|\tan(\phi_i)|}{\sqrt{vx_i^2 + vy_i^2}}$ and c_x and c_y are constants



Alerting Logic in ALAS

- *Alerting Logic* - projects the behavior of intruder
- Considers 3 possible scenarios
  1. Bank angle $\phi_i = 0$
  2. Known bank angle ϕ_i
  3. Maximum bank angle ϕ_{max}
- t_i and t_o – time taken to reach point of intersection
- $Alert_\pi(x) \equiv t_i > t_o$ *then* $\Delta t^2 \times (vx_i^2 + vy_i^2) < Back^2$
  else $\Delta t^2 \times (vx_i^2 + vy_i^2) < Front^2$



- Temporal precedence property to be checked

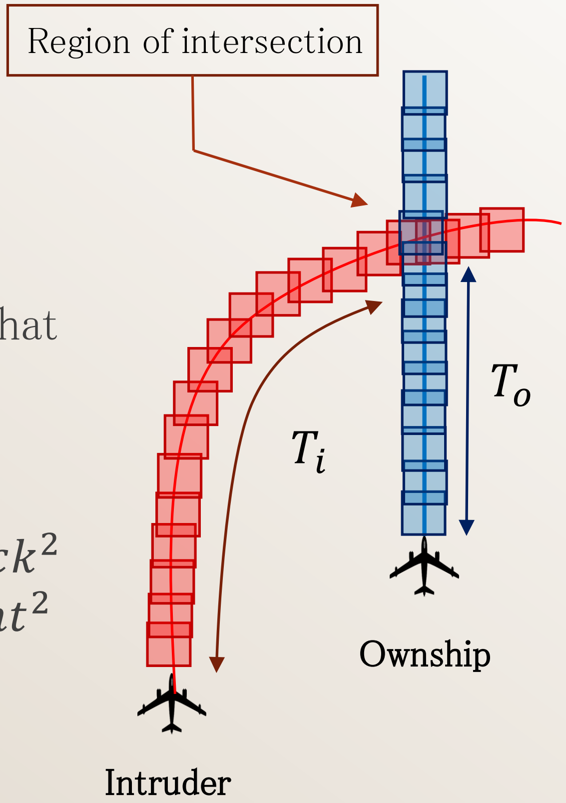
$$\boldsymbol{Alert} \prec_b \boldsymbol{Unsafe}$$

Alerting Logic in ALAS

- t_o and t_i – closed form solutions involve exponentials
- Compute intervals T_i and T_o from *ReachTubes*, such that $t_i \in T_i$ and $t_o \in T_o$
- $Alert'_\pi(x) \equiv T_i > T_o$ *then* $\Delta T^2 \times (vx_i^2 + vy_i^2) < Back^2$ *else* $\Delta T^2 \times (vx_i^2 + vy_i^2) < Front^2$
- Temporal precedence property verified

$$\boldsymbol{Alert' \prec_b Unsafe}$$

- Guarantees soundness and relative completeness



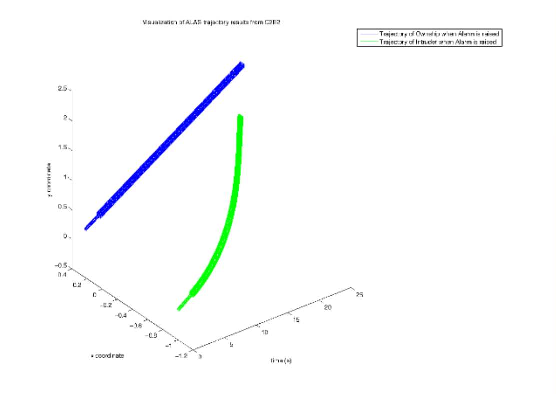
Verification Results

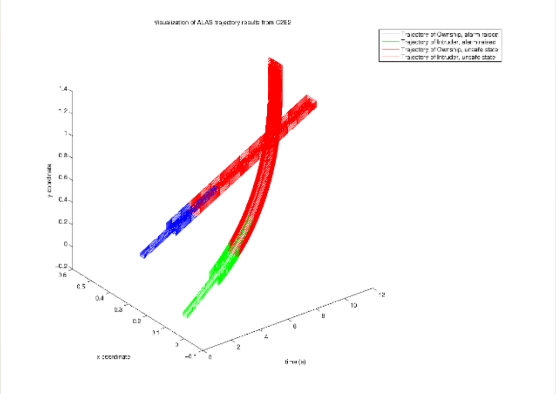
- Running times for several cases terminates in minutes
- Compute b such that $\boldsymbol{Alert} \prec_b \boldsymbol{Unsafe}$ is satisfied
- When property is not robustly satisfied, then verification might not terminate

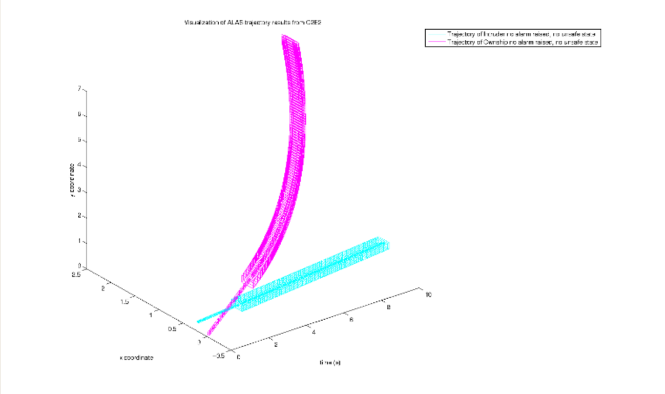
Scenario	Alert $\preccurlyeq_4$ Unsafe	Time (mins:sec)	Alert $\preccurlyeq_?$ Unsafe
6	False	3:27	2.16
7	True	1:13	–
8	True	2:21	–
6.1	False	7:18	1.54
7.1	True	2:34	–
8.1	True	4:55	–
9	False	2:18	1.8
10	False	3:04	2.4
9.1	False	4:30	1.8
10.1	False	6:11	2.4

Verification Results – Interesting Scenarios

- *Flase Alert* - safe separation is always maintained and alert is raised
- *Missed Alert* - safe separation is violated, but alert is not raised
- *No Alert* - separation among aircraft is always maintained and alert is not raised







Conclusions and Future Work

- Presented a verification technique for temporal precedence properties
- Verifying *guarantee* predicates
- Applied it to ALAS for discovering interesting scenarios such as *false alerts* and *missed alerts*

Future Work:

- Additional complexities in behavior of intruder and ownship
- Verifying collision avoidance maneuvers

Conclusions and Future Work

- Presented a verification technique for temporal precedence properties
- Verifying *guarantee* predicates
- Applied it to ALAS for discovering interesting scenarios such as *false alerts* and *missed alerts*

Future Work:

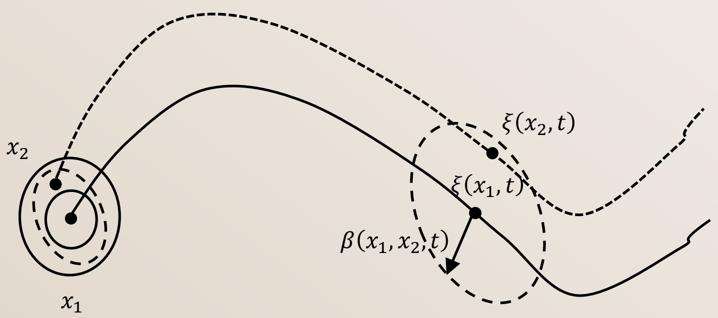
- Additional complexities in behavior of intruder and ownship
- Verifying collision avoidance maneuvers

Questions?

Annotations: Discrepancy function

- Definition. A smooth function $\mathrm{V} : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{\geq 0}$ is a *discrepancy function* for $\dot{x} = f(x,t)$ if for any x_1 and $x_2 \in \mathbb{R}^n$
    1. (static bound) $\exists\ \alpha_1, \alpha_2$: $\alpha_1(|x_1 - x_2|) \leq V(x_1, x_2) \leq \alpha_2(|x_1 - x_2|)$
    2. (dynamic bound) $\mathrm{V}\big(\xi(x_1,t), \xi(x_2,t)\big) \leq \beta(x_1, x_2, t)$ where $\beta: \mathbb{R}^{2n} \times \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ and $\beta \rightarrow 0$ as $x_1 \rightarrow x_2$

- $(\alpha_1, \alpha_2, \beta)$ is a witness for V



- Stability not required

- Multiple annotations for the same system

Contraction Metrics

- Definition. A positive definite, symmetric matrix M is a contraction metric for the system if $\exists\, \beta_M \geq 0$ such that $\frac{\partial f}{\partial x}^T M + M \frac{\partial f}{\partial x} + \beta_M M \preccurlyeq 0$

- Theorem. [Lohmiller & Slotine`98]. If M is a contraction metric then $\exists\, k \geq 1, \gamma > 0$ such that $\forall\, x_1, x_2, t,\ |\xi(x_1, t) - \xi(x_2, t)|^2 \leq k|x_1 - x_2|^2 e^{-\gamma t}$

- Proposition. $|x_1 - x_2|^2$ is a discrepancy function with $\beta \coloneqq k e^{-\gamma t}|x_1 - x_2|^2$

Incremental Stability

- Definition. The system is incrementally stable if there is a KL function γ such that for any two initial states $x_1$and x_2 $|\xi(x_1, t) - \xi(x_2, t)| \leq \gamma(|x_1 - x_2|, t)$.

- Theorem. [Angeli 2000]. If the system is incrementally stable then there exists a smooth function (incremental Lyapunov function) $\mathrm{V}: \mathbb{R}^{2n} \rightarrow \mathbb{R}^{\geq 0}$ and $\alpha: \mathbb{R} \rightarrow \mathbb{R}^{\geq 0}$ s.t.

$$\mathrm{V}\big(\xi(x_1, t), \xi(x_2, t)\big) - V(x_1, x_2) \leq \int_0^t -\alpha(|\xi(x_1, \tau) - \xi(x_2, \tau)|) d\tau.$$

- Proposition. Incremental Lyapunov function is a discrepancy function with

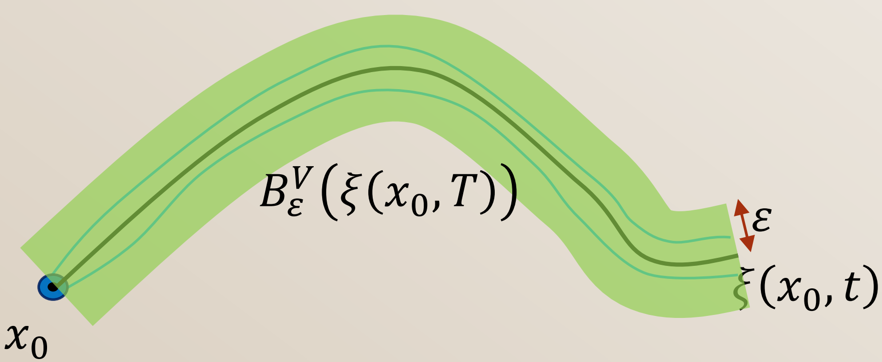
$$\beta(x_1, x_2, t) = V(x_1, x_2) + \int_0^t -\alpha(|\xi(x_1, \tau) - \xi(x_2, \tau)|) d\tau.$$

About Annotations

- How are annotations useful : computing sound over approximations

$\forall\, x \in B_\delta(x_0), \xi(x,T) \in\ B_\varepsilon^V\big(\xi(x_0,T)\big)\ where\ \varepsilon = \sup_{x\, \in B_\delta(x_0), 0\le t\le T} \{\beta(x,x_0,t)\}$

$B_\varepsilon^V(x) = \{\, x' \,|\, V(x,x') \le\ \varepsilon\}$



Alert Predicate Closed Form

- $dir = sign((x_o - x_i) \times vy_i - (y_o - y_i) \times vx_i)$
- $r = \frac{\sqrt{vx_i^2 + vy_i^2}}{\omega}$; $c_x = x_i + dir \times \frac{vy_i}{\omega}$; $c_x = y_i + dir \times \frac{vx_i}{\omega}$
- $if \left(r^2 \times (vx_o^2 + vy_o^2) - \left((x_o - c_x) vy_o - (y_o - c_y) vx_o \right)^2 \right) < 0$; $Alert = 0$
- $M = (x_o - c_x) vx_o + (y_o - c_y) vy_o; N = \frac{1}{r^2}((x_o - c_x)(x_i - c_x) + (y_o - c_y)(y_i - c_y))$
- $t_o = \frac{1}{vx_o^2 + vy_o^2}\left[-M + \sqrt{(M^2 - vx_o^2 + vy_o^2)((x_o - c_x)^2 + (y_o - c_y)^2 - r^2)}\,\right]$
- $t_i = abs\left(\frac{r}{dir \times \sqrt{vx_o^2 + vy_o^2}} \times \text{acos}(N)\right)$
- $if\,(t_o > t_i \wedge (t_o - t_i)^2 \times (vx_o^2 + vy_o^2) < Front^2)$; $Alert = 1$
- $if\,(t_i > t_o \wedge (t_o - t_i)^2 \times (vx_o^2 + vy_o^2) < Back^2)$; $Alert = 1$